CUSTOMIZABLE CRYPTOGRAPHIC DEVICE

Russell D. Housley
Gregory W. Piper
Randy V. Sabett

> This application is a continuation of application now 09/013,821 filed on January 27, 1998

4/28/05

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to cryptographic devices and, in particular, to a cryptographic device that can easily, securely and/or irreversibly be customized to provide specified cryptographic functionality.

2. Related Art

A "cryptographic device" is a device which can be used to perform cryptographic operations on data. Examples of cryptographic operations include key exchange operations, hash operations, digital signature operations, symmetric encryption (secret key) operations, asymmetric (public key) encryption operations, and key wrapping operations (for both symmetric and asymmetric keys). A "cryptographic characteristic" is an attribute of the manner in which a cryptographic operation is performed. An example of a cryptographic characteristic is the length of a cryptographic key. The cryptographic operations and cryptographic characteristics of a cryptographic device are sometimes referred to herein as the "cryptographic functionality" of the cryptographic device. The cryptographic functionality of a cryptographic device can be implemented by a computer processor executing instructions and/or accessing data stored on a data storage device. Herein, such instructions and/or data are sometimes referred to, singly or collectively, as "code."

FIG. 1 is a block diagram of a typical way of producing and using a cryptographic device. Initially, as shown by block 101, a cryptographic device is "produced." As used herein, at the end of "production" of a cryptographic device,